Case study of Lykke exchange: architecture and outlook

Olsen, Richard ; Battiston, Stefano ; Caldarelli, Guido ; Golub, Anton ; Nikulin, Mihail ; Ivliev, Sergey

DOI: https://doi.org/10.1108/JRF-12-2016-0168

Received 22 December 2016
Revised 11 August 2017
Accepted 24 September 2017

Case study of Lykke exchange: architecture and outlook

Richard Olsen
Lykke Corp, Zurich, Switzerland

Stefano Battiston
Department of Banking and Finance, Zurich, Switzerland

Guido Caldarelli
IMT Alti Studi Lucca, Lucca, Italy

Anton Golub and Mihail Nikulin
Lykke Corp, Zurich, Switzerland, and

Sergey Ivliev
Department of Economics, Perm State University, Perm, Russian Federation

Abstract

Purpose – This paper aims to explain the architecture and design choices of the exchange. Lykke is a FinTech company based in Zurich that has launched the global marketplace for all asset classes and instruments digitized on the blockchain. The authors discuss how the exchange will evolve over time. They explore the macroeconomic benefits of the new blockchain technology. The Lykke exchange is compatible with any type of public blockchain.

Design/methodology/approach – The authors present the architecture of an exchange for colored coins. By colored coins, they mean issuer-backed securities on the Bitcoin blockchain. Orders are collected and matched by a semi-trusted exchange. Matched orders are settled on the Bitcoin blockchain, where each successful trade between parties appears as a set atomic-colored coins swap transactions. Unfilled and expired orders are discarded. The exchange does not take possession of the traded coins, but needs to be trusted to match trades correctly.

Findings – Lykke has launched the exchange initially for the main currencies, cryptocurrencies and Lykke coin (entitlement to the shares of Lykke company). Perspective asset classes include futures and options on digital assets, crowd-funded loans for retail and private equity financing for small and medium-sized enterprises, contracts for difference, zero coupon bonds and other fixed income and natural capital bonds.

Originality/value – Lykke exchange and all its tools and services are open source; the transparency of technology is ideal for research. The paper provides a high-level overview of the exchange and concludes with a research agenda.

Keywords Blockchain, Alternative trading systems, Coloured coins

Paper type Case study

1. Introduction

The financial system architecture has grown organically. Over the past 40 years, individual steps of the workflow of financial transactions have been computerized; the business process remained unchanged, as if processing continued to be manual. Delivery and settlement of transaction is batch based and occurs with a time delay of two and more days and does not happen at the time of the trade. The outcome is a convoluted banking architecture, a pile of spaghetti. Every bank has its own bookkeeping system and is an

The Journal of Risk Finance
Vol. 19 No. 1, 2018
pp. 26-38

1526-5943
DOI 10.1108/JRF-12-2016-0168

island from an audit point of view, where verification of trades is cumbersome and prone to errors. This regime contributes to a high degree of fragmentation and uncertainty in the market, multiplication of risk factors, high transaction costs for financial assets and lack of liquidity and transparency in financial markets.

In attempt to rewire the current financial system, Lykke builds a global internet exchange, where all financial instruments will be traded and exchanged against each other, whatever their asset class or the size of transaction. Every financial instrument will be a listed security in the form of a digital token and all transactions will be logged in a universally accessible distributed ledger, a decentralized notary service that ensures immediate global consensus about completed transactions and asset ownership. Like the internet itself, the ledger is not controlled by a single entity, but an emergent phenomenon consisting of its participants. Trades will be settled and validated immediately; processing will be digital and transaction costs will be minuscule. The ledger includes a wallet, so that every owner of a digital coin has his own private key protecting his ownership. There will be an intraday interest rate market and yield curve. Market participants will be able to buy and sell colored coins of different issuers and change counterparty risk at any time. The number of traded financial instruments will grow exponentially, transaction volumes will skyrocket and liquidity will be ample.

Lykke aims to become the global marketplace and establish itself as the backbone of a new and highly sophisticated banking architecture that is not plagued by the deficiencies of the present system. This paper introduces the architecture of Lykke exchange and provides the details on the first months of trading.

2. Blockchain and colored coins

Blockchain is a way to find a consensus among a multitude of servers in the absence of mutual trust. Most blockchain variants follow a proof-of-work protocol, which provides strong economic incentives for contributing to the network security (mining).

Open blockchain is a great platform to build other services on top, as it is an independent technology without any vendor lock-in or other entity behind it that might abuse it one day to further their strategic agenda. Examples of other such open decentralized technologies that serve as a platform for others to build on are Linux, email or the internet. A blockchain should be the technology of choice for projects that benefit from high inter-operability and versatility in use.

As soon as the involved parties can be trusted, there are usually more efficient solutions than a distributed ledger. When the main issue is unreliable hardware that can otherwise be trusted, the Paxos algorithm is typically used. This is what Google does to provide reliable services with commodity hardware. Then, there are multiple database solutions that can be the most efficient in principle but require highly reliable hardware and also complete trust in the operator. Decentralization comes at a cost.

Open platform technologies can unleash enormous powers, which would not materialize in a centralized setup. The classic example is the internet, which thrives because of its open architecture and which has quickly outrun all alternative approaches (e.g. the French Minitel). Another example is Linux, which serves as an operating system for the majority of servers in the internet. Its main advantage is the fact that a company can commit to using it without becoming dependent on a potential competitor. A third example is the email protocol, which is being used to send billions of messages every day. Email would never have flourished to the same extent if it was directly controlled by a company. Similarly, Bitcoin (Nakamoto, 2008) is often seen as the open platform for finance.

Originally, Bitcoin was most popular among cypherpunks and crypto-anarchists. To this day, Bitcoin has a significant number of proponents from that background, who love Bitcoin for its libertarian philosophy and who cherish it as digital gold. Driven by a vast inflow of venture capital, Bitcoin is gaining broader traction among early adopters whose enthusiasm stems more from Bitcoin's usefulness and versatility than from its technical brilliance.

Since 2014, Bitcoin saw unprecedented inflows of venture capital. It is one of a number of growing startups that have each raised venture capital in the double digit millions. While most Bitcoin startups are profit-driven with a clear plan for generating revenue, Blockstream which recently raised 21 million is a remarkable exception. Unlike other Bitcoin startups, Blockstream aims at improving the Bitcoin infrastructure itself – without obvious financial benefit. Its investors argue that there is huge value in being able to help shaping the future of the Bitcoin protocol and being at the forefront of Bitcoin development.

Given the price estimates of the current mining hardware[1], it would cost above USD300 million in hardware to acquire enough computing power to dominate the Bitcoin network.

Initially, enthusiasts and hobbyists with desktop PCs and later graphics cards equipped with parallelized chip architecture did Bitcoin mining. Today, Bitcoin mining has become a professional endeavor, with custom-designed chips and a value chain of specialized services. Hardware manufacturers such as Bitmain Technologies or BitFury design and manufacture specialized ASIC chips. The miners operate the hardware – typically in locations with low electricity costs and sell the generated computing power to mining pools, which, in turn, redistribute the freshly minted coins and earned transaction fees back to the miners.

The Bitcoin blockchain is currently the largest blockchain in operation. The hardware cost to match the computing power that currently secures the Bitcoin blockchain is likely in the triple-digit millions, if not higher. When measuring security as the USD cost of an attack, the most secure blockchain currently in existence is the Bitcoin blockchain. There are alternative cryptocurrencies that add security in principle thanks to certain tweaks. Litecoin, for example, uses a hashing algorithm that makes it harder to create specialized mining chips. Ethereum follows a plan to discourage a professionalization in mining and switch to the proof-of-stake consensus model. But the sheer amount of computing power securing the Bitcoin blockchain dwarfs the effect of those tweaks. One cannot rule out that other cryptocurrencies succeed at taking the lead security-wise in the medium-term future, but for now, the Bitcoin blockchain remains the most secure platform to build on.

The value of a currency strongly depends on the number of participants[2], which, in turn, attracts more participants, leading to a network effect. Thus, Bitcoin has a significant first-mover-advantage, which plays out threefold:

- The more users there are, the more useful Bitcoin becomes, as there are more places to spend Bitcoin and counterparties to exchange Bitcoin with, attracting even more users.
- Currencies require trust, but trust can only be built over time, thus – everything else equal – giving the oldest currency a natural edge over its competitors.
- The more volume there is, the more transaction fees there are, attracting more miners and making the network more secure, which, in turn, again attracts additional users and volume.

With currencies that serve as a store of wealth, there is an additional lock-in insofar as it is takes effort to transfer that wealth into other currencies. Thus, there are multiple effects in place that make it very hard to dethrone Bitcoin.

Every financial instrument can become a listed security on the blockchain in the form of a digital token: on Bitcoin blockchain, it is implemented through the various Colored Coin protocols (Open Asset, Colu, etc.). Colored coins (Rosenfeld, 2012) follow the idea of "coloring" a specific Bitcoin – the issuer guarantees to hand out the underlying assets to the person, who returns the colored coin. For example, the Federal Reserve (FED) can issue a colored coin in the same way as it prints paper money; it would take a fraction of a Bitcoin and then insert the "I Owe You" statement of the FED, like a regular bank note. The same mechanism can be used for any other financial claim. Colored coins are different in nature than cryptocurrencies because they have a specific issuer and are backed by a real financial asset.

Reporting of colored coins in traditional banking software systems, such as bookkeeping and risk management is straightforward because every colored coin can include an International Securities Identification Number (ISIN), thus can be treated as any other financial instrument, fully compatible with existing back-office systems. Financial institutions can create colored coins for existing financial products and gradually move business processes to blockchain. They can operate the old and new system in parallel and switch over to the new system at their own pace. In the new system, interest rate payments are second by second improving liquidity provision.

The criticism of the colored coin approach, summarized in Swanson (2015), includes the inability of the miners to validate the colored coin transaction (Bitcoin mining pools are not color aware), difficulty for governmental organization to enforce sanctions in a public blockchain, probabilistic settlement finality and excessive transparency of the public blockchain.

The advantages of using Bitcoin blockchain as a ledger for asset tokenization leverage its immutability, non-counterfeitability, ease of transfer, robustness and transparency and protection from double spending. The issuer risk still exists – colored coins are as good as its issuer.

2.1 Summary

To summarize, Bitcoin is one of those technologies in which people see the potential to disrupt the world. It illustrates the power that open platforms can unfold. There are various competitors and clones, but none of them comes close to the popularity and success of Bitcoin. The many unsuccessful attempts of creating competing coins show that one should, whenever feasible, ride the wave and build on top of Bitcoin instead of creating one's own proprietary ledger. By building on top of Bitcoin, one can leverage the power if its blockchain, which has been continuously running for over six years and amassed computing power worth hundreds of millions, thereby enabling a lean business model that stands on the shoulders of a giant.

3. Colored coins exchange architecture

We present the architecture of an exchange for colored coins. By colored coins, we mean issuer-backed securities on the Bitcoin blockchain. Orders are collected and matched by a semi-trusted exchange. Matched orders are settled on the Bitcoin blockchain, where each successful trade between parties appears as a set atomic-colored coins swap transactions. Unfilled and expired orders are discarded. The exchange does not take possession of the traded coins but needs to be trusted to match trades correctly. Assuming a basic level of trust in the trader – which could, for example, be established by providing collateral – trading can take place as fast as the communication between trader and exchange permits, with a subsequent settlement on the blockchain.

3.1 Design considerations

Exchanges for cryptocurrencies can be organized with a different degree of centralization. Typically, centralized exchanges are much more efficient, whereas decentralized exchanges are more secure, as they require less trust in the exchange. Owing to their higher efficiency and simplicity, most volume is currently traded on centralized exchanges such as BTC China, Bitstamp or Bitfinex[3]. A trader on such an exchange must entrust all assets in his trading account to the exchange. History shows that this is not without risk, with the most famous examples being the collapse of MtGox (more than 600,000 Bitcoins disappeared) and the most recent hacking of Bitfinex (120,000 stolen Bitcoins). Exchanges such as Bitcoin.de and LocalBitcoins are more decentralized and restrict themselves to organize trades and offer escrow services, but let the traders execute the actual trade bilaterally, whereas traders on LocalBitcoins often even meet physically. This naturally limits the achievable speed of trading to the speed of the underlying payment system (e.g. SEPA or moving bank notes). These exchanges can achieve a much higher trading frequency without having to resort to client deposits by restricting themselves to cryptocurrencies that can be exchanged instantly. Examples of such exchanges or whole cryptocurrency systems that include built-in decentralized exchanges are Omni, Counterparty and BitsharesX – none of which achieved the same commercial success yet as the aforementioned centralized exchanges. These exchanges frequently try to even decentralize the matching of trades, which is problematic, as it is fundamentally hard to enforce rules in a decentralized system, especially when timing is crucial. For the design of our exchange, we opt for a system with centralized matching of trades, but with direct bilateral exchange of assets, trying to combine the best of both worlds (see the comparison of Lykke exchange with the other types of crypto-exchanges in the Table I). One should also note that, when trading a particular colored coins or any other issuer-backed asset, there is exposure to a centralized point of failure anyway, namely, the issuer.

We follow the design principles of simplicity and minimal risk. Thus, we prefer proven systems with known shortcomings that are good enough for our purposes over theoretically better systems. The best validated blockchain is clearly Bitcoin, with a blockchain spanning back more than five years. Unfortunately, the Bitcoin network only supports one asset, the Bitcoin. One way to overcome this would be to create an adapted version and to operate a separate blockchain that runs that adapted protocol. With a separate blockchain, one cannot benefit from all the computing power securing the Bitcoin network, calling for further adaptions, such as abandoning proof-of-work (majority of computing power says which transactions settle) for proof-of-stake (majority of coin wealth says which transactions settle) or something entirely different. The path of building a custom ledger has been chosen by a number of cryptocurrencies, such as Ethereum. This leads to the risks of over-engineering and stepping into uncharted territories, which are both hard to control.

Thus, instead of creating yet another distributed ledger, we decided to make use of the colored coins approach, which builds on top of the Bitcoin blockchain. As the name suggests, colored coins follow the idea of "coloring" a specific Bitcoin, with an issuers guaranteeing to hand out the underlying assets to whoever returns that colored Bitcoins (or a fraction thereof). Thus, such colored coins are always linked to Bitcoins – like physical coins being bound to a few grams of a metal that also has a value in itself and is independent of the currency value. Further limitations are discussed in the scalability section. Current implementation of the Lykke exchange operates with Open Asset colored coins protocol[4].

The proposed exchange is positioned in between completely decentralized proposals (such as Counterparty) and completely centralized ones (such as Bitstamp). Decentralized approaches tend to come with significant overhead, for example, by creating an entry on the

Criteria	Centralized exchanges	Decentralized exchanges	Semi-centralized exchanges
Examples	Bitfinex, Poloniex, Kraken, Bitstamp	0x, EtherDelta, Counterparty, BitsharesX, LocalBitcoins, Bitcoin.de	Lykke
Trust	User entrusts all assets in his trading account to the exchange	User does not entrust the assets to the exchange	User does not entrust the assets to the exchange
Privacy	Users are required to disclose their personal details	Users are not required to disclose their personal details, except if the exchange method involves bank transfers	Users are not required to disclose their personal details, except if the exchange method involves bank transfers
Risk of hacks	High (because the exchange controls all the funds)	Low (because of the direct ownership on the funds)	Low (because of the direct ownership on the funds)
Centralized matching engine	Yes	No	Yes
Speed of transaction execution	Fast (because of the centralized matching engine)	Slow	Fast (because of the centralized matching engine)
Advanced trading functionalities (like margin trading, lending and stop loss)	Easy to implement (because of the centralized matching engine)	Very difficult (or even impossible) to implement	Easy to implement (because of the centralized matching engine)

Table I. Comparative analysis of the exchanges with different degree of centralization

blockchain for every issued order. Centralized exchanges are much more efficient, but require the exchange to take possession over the assets of the traders as deposits, which in many jurisdictions comes with certain regulatory duties (e.g. requiring a banking license). Our approach finds a middle ground between those two. Only completed trades enter the blockchain, while unfilled orders are discarded. At the same time, assets can be traded *ad hoc* and are directly transferred between the trading parties, thereby letting the exchange act as a mere broker without clients' deposits.

There are three involved parties:

(1) Issuers issue IOUs as colored coins. These coins can represent currencies, stocks or any other transferable asset. An exchange can demand from the issuer to file a formal application for his coins to be listed, but there is no technical necessity to do so. In principle, any colored coins could be traded on an exchange – even without the consent of the issuer. The role of the issuers is passive; all they can do is observing completed trades as they settle on the blockchain.

(2) Traders possess Bitcoins or colored coins and desire to trade them for other assets. Traders typically need to be registered with the exchange to establish a basic level of trust (e.g. legally or by providing a collateral). To initiate trades, they send orders to an exchange of their choice. The traded assets must reside on a Bitcoin address associated with the trader's account on the exchange. Traders primarily communicate directly with the exchange, but should also observe the blockchain to verify the correct settlement of their trades.

(3) Exchanges wait for traders to send them orders and collect them in an order book. The usual order types are supported (bid, ask, limit, etc.). Matched trades are settled on the blockchain. In principle, any asset pair can be traded, but in practice, market forces will probably let a dominating currency emerge (similar to the US dollars in classical foreign exchange). There could be various competing exchanges.

3.2 Design description

Traders create an order by creating and signing a collateral transaction to send x coins to the exchange, whereas x is the amount and type of coins they intend to sell. Unlike usual transactions, this collateral transaction is not sent to the Bitcoin network, but to the exchange instead, along with additional information about the order (type, asset to buy, limit, etc.). The collateral transaction guarantees settlement for the matched trade in case if trader is offline. The provided collateral transaction will never be broadcasted over the Bitcoin network if client signs atomic swap transaction for the matched trade. As soon as the exchange receives a matching order containing a second collateral transaction, the exchange creates an atomic swap transaction that sends the exchanged amounts to the two traders and asks both traders to sign it. Broadcasting of the atomic swap transaction signed by both traders will invalidate guarantee transactions, while it is spending the same outputs. If one of the trader is offline and not able to sign, the swap transaction exchange uses collateral transactions and sends the exchanged amounts to the two traders. Unfilled or cancelled orders are simply discarded.

3.3 Partial trades

Most of the time, one of the involved orders will only be partially filled. The remaining funds are immediately returned to the sender for resubmission of the remaining trade. For example, if trader Toni issues an order to sell USD100 for Euros and his order is immediately matched with USD80 worth of counter-orders, the remaining USD20 are sent back to Toni along with the acquired Euros. Toni's trading software then automatically creates and signs a new order to sell the remaining USD20.

3.4 Matching engine with price-spread-time priority

Lykke exchange implements a new type of queuing system for the limit orders. The queuing system is price-spread-time dependent because it rewards market participants for quoting two-way prices and revealing information about their price expectation. Market participants who are confident that the price level will remain unchanged, will offer low spreads, they will get preferential treatment and will move ahead in the queue. High-frequency traders will not be able to extract an unfair advantage from the pending limit orders as is the case today with price-time queuing systems that are standard. The innovation translates into improved price discovery with lower price volatility and improved market efficiency. The price-spread-time queuing system is a major innovation for the industry of electronic market places, which use queuing systems that are only price-time dependent.

3.5 Multisignature wallets

To be able to trade, traders should deposit coins into exchange. Depositing coins is not equal to trusting coins. Exchange uses 2-of-2 multisignatures address wallets to deposit trader's

coins. 2-of-2 multisignature address requires two signatures to spend coins from it – both trader's and exchange's signatures (Figure 1).

MultiSig wallet provides the following advantages:

- *Deposit does not mean trust*: Exchange cannot spend coins without trader's key. Even if the exchange is compromised and the exchange's key is stolen, the trader will not lose his coins. The second key is required to spend deposited coins.
- *Coins flow control*: On the other hand, exchange's signature is required for each transaction. Deposited coins cannot be transferred outside the exchange without exchange being aware of it.
- *Green nodes network*: Identified clients only (KYC) are allowed to trade. A trader is able to spend deposited coins whether for trading inside the exchange or for withdrawal. A trader cannot transfer the coins outside the exchange green nodes network if it's not allowed by the issuer.

What happens with deposited coins if exchange's private key is destroyed? Would the deposited coins be frozen in the multisignatures address forever? To guarantee funds recovery from the MultiSig wallet, exchange provides offchain refund transactions (Figure 2).

Refund transaction sends deposited coins back to the trader's private address. Once the refund transaction is signed by exchange and trader, the refund can be broadcasted after 31 days. The refund transaction is invalidated each time when the trader makes a trade that spends "refunded" outputs. Exchange generates a new refund transaction after each new trade and sends the transaction binary file to the trader's mail. The trader may use the refund in case of emergency.

Exchange monitors new transactions on the blockchain and detects if the valid refund transaction was broadcasted. It is considered as withdrawal.

Note: Two signatures are required to spend coins – both trader's and exchange's

Figure 1.
2-of-2 Multisignature address used to deposit trader's coins

Note: Refund transaction will be valid after 31 days lock

Figure 2.
Off the blockchain refund transaction is signed by the exchange

3.6 Settlement capacity

Generally, all received coins can immediately be reused in a new trade. Thus, trading can be as fast as the connection between trader and exchange permits (normally in the range of 10-100 ms). Temporarily, the number of trades can exceed the limits given by the Bitcoin blockchain, as this just leads to a delayed settlement. Note that the size of the collateral (or amount of trust in the trader) should cover the potential net gain of the trader when unwinding the unsettled transactions. Thus, the exchange should measure that potential net gain and block further trading in case it approaches the size of the collateral.

Upon the implementation of recent SegWit soft-fork, the Bitcoin network will have a limit of about 780,000 transactions per day[5]. Today, the network processes about 200,000 transactions per day[6]. As soon as the number of issued transactions hits the limit, miners will start to drop the ones with the lowest fees. As every dropped transaction means a loss of potential revenue, they will likely push for an increase of the limit in such a scenario. The actual technical limit according to core developer Gavin Andresen is in the range of hundreds of millions of transactions per day[7].

To mitigate capacity limit, Lightning Network[8] (Poon and Dryja, 2016) and Micropayment channels[9] are the perspective approaches. Instead of broadcasting of each single transaction on the blockchain parties deliver coins by sending signed transaction messages offchain with subsequent net settlement on the blockchain.

3.7 Micropayment channels approach

Micropayment channel is based on the 2-of-2 multisignature address where both parties of the channel deposit coins into the address and communicate off the blockchain. The current balance of parties is stored as the most recent offchain refund transaction signed by both parties, spending from the multisignature address. Bitcoin Opcode OP_CHECKSECVENCEVERIFY (BIP-0112) is available for relative lock-time on mainnet Bitcoin blockchain from May 2016. This opcode can be used for providing revocable refund transaction for the multisignature payment channel address[10]. To make a transfer, client sends a signed refund transaction message spending the corresponding volume of coins from the multisignature address. The final refund transaction signed by both parties can be broadcasted when the parties withdraw their coins.

3.8 Payment Hubs

Payment Hub acts as an intermediary for transferring money from one point to another. Traders who need to exchange an asset in a scalable way would open micropayment channels with Payment Hubs. When one wants to send US dollar coins to the exchange he/she would send coins to the US dollar Payment Hub using the channel, then the hub sends its coins to the exchange using another channel. Payment Hubs cannot steal coins on the way to exchange because of using hash lock protection[11]. Payment Hubs provide coins in the payment channel address for being able to route payments effectively. Exchange sends Euro coins back to the trader using another Euro Payment Hub that provides liquidity for the Euro coins. Issuers of coins may act as Payment Hubs to provide transferring of the issued coins in the scalable way (Figure 3).

3.9 Attacks

Malicious traders could prevent the settlement of a trade by issuing a competing transaction that sends the offered coins elsewhere. Doing this is trivial as long as the order is pending and thus no transaction published – but assuming that the exchange provides an option to

cancel pending orders, there is no motivation to do so as both result in the same, namely, the cancellation of the order.

A malicious trader might also regret an order after it was matched and sent to the network, thus wanting to disrupt settlement. As transactions spread quickly through the Bitcoin network, successfully issuing a competing transaction to prevent that regretted trade would require collusion with the miner who happens to mine the next block – something a large mining pool probably would not want to risk its reputation for as such cheating attempts are perfectly detectable. The easy detectability also allows to automatically trigger counter-measures such as freezing the collateral of the trader or banning the trader.

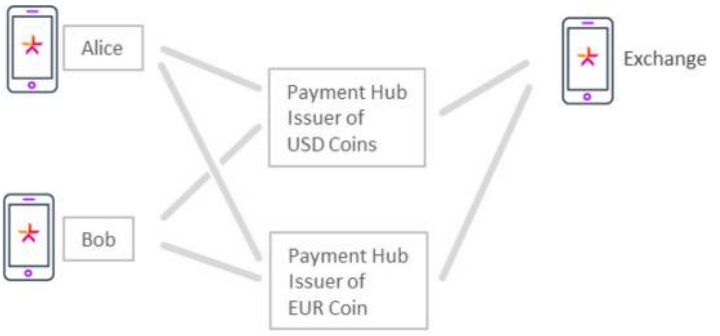
A related attack is based on transaction malleability. Transaction malleability is a weakness in the Bitcoin protocol that allows anyone to slightly alter a transaction in ways that cause the transaction to change its id (hash). Should the altered transaction enter the blockchain instead of the original one, already issued follow-up transactions will be orphaned and fail, as they use the original ID to refer to their predecessor. The necessary adaptations to the Bitcoin protocol to fix this are known and implemented.

Another attack on the system could be performed by the exchange itself. If hacked or run by a malicious operator, whoever controls the exchange could potentially take possession of all assets in all currently pending orders. This is already much better than the risk of traditional exchanges like MtGox to misappropriate all their clients accounts, but is still a significant risk that needs to be addressed through according security and regulatory measures.

All the aforementioned risks pale in comparison to the counterparty risk inherent in colored coins. Regardless of how securely the exchange is organized, an issuer of colored coins could default or misappropriate the underlying assets. An exchange can help to alleviate this risk by only, allowing the trade of coins from verified issuers with quantifiable counterparty risk. This risk can be mitigated by diversifying coins across multiple issuers and by swapping to coins that are deemed less risky if necessary.

3.10 Leveraged trading

To provide leveraged trading, an intermediary service such as a bank willing to provide credit is necessary. This is basically the same as traditional leveraged trading. Instead of directly trading on the exchange with their own wallets, traders will transfer their assets to a managed wallet. Such a managed wallet resembles a bank account, with the bank managing the wallet having full control over the contained assets. Like in classical banking, orders issued by the traders go to the bank first, where they are verified, and then sent to the



Note: Issuer of the coins may act as payment hub

Figure 3.
Both exchange and traders have micropayment channels with payment hubs to be able to transfer multiple types of coins off the blockchain

exchange. The bank can then offer credit to the trader, which is added to the managed account. But as soon as the account is not sufficiently covered any more, the margin call is issued, the assets liquidated, and outstanding credit returned to the bank.

3.11 Information technology architecture

The Lykke exchange was developed since December 2015 and went live beta on March 2016 with wider industry test started in May 2016. The infrastructure consists of the following components:

- Matching engine;
- Lykke backend (Microsoft Azure);
- Blockchain of Bitcoin/Open Asset colorcore;
- Issuer UI;
- Lykke Wallet app (iOS/Android); and
- Market making algorithms.

Lykke exchange and all its tools and services are fully open source[12]. Total size of Lykke code in Github repository has recently reached 3.3 mln lines, with own (not-forked) code exceeding 3 mln (Figure 4).

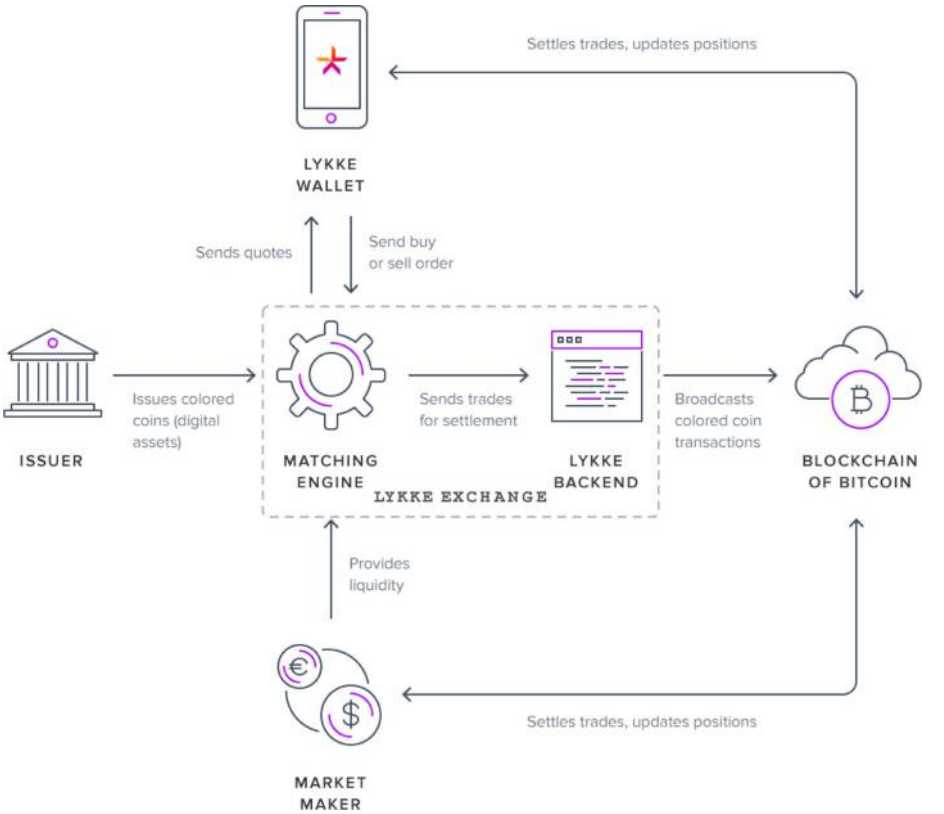


Figure 4.
Lykke exchange high-level architecture

The development process has started as a result of a competition launched in September 2015. Three prizes were awarded to the three submissions that were received. The proposed projects were complementary to the design of FX platform and the asset protocol, and this helped to form a core of the Lykke team.

3.12 Crowd-based approach to resources

The company organization is inspired by the principles that govern dynamic systems in nature, such as the human body. Lykke implements an emergent structure, where processes are crowd-based and contributors are incentivized with prizes in many different shapes and forms. Prize-payouts have a scaling property with many small prizes. The scaling property of prizes reward many individuals and nurture talent on a broader scale than the typical approach of just offering one first, one second and one third prize. We successfully applied this idea in the design competition for the exchange.

The company has a small core group of managers; they are mandated to get the processes going, fine tune operations or have very specific technical expertise. We use the crowd process as a screening mechanism to identify highly dedicated and gifted employees. The crowd-based management principle has to our knowledge never been implemented as radically as envisioned for Lykke. There are, however, examples of companies and non-profit organizations that have followed similar management principles, such as Wikipedia, Mozilla or Open Source Initiatives, such as Bitcoin or Eclipse. The productivity of these initiatives in terms of output relative to cost is an indication that the crowd-based strategy may surpass expectations.

3.13 Summary

Building a secure, high-performance exchange for colored coins is technically feasible. There is a number of trade-offs between performance and security. In a trusted environment, the highest performance is reached, whereas a completely secure setup comes at a price of slower transactions. Both approaches can be mixed depending on requirements. Blockchain technology allows to run such a crypto-exchange in a fully transparent and open way, potentially allowing for anyone to trade on it with minimal trust requirements and providing a platform for other crypto-services to build on. Current implementation of the Lykke exchange operates with Open Asset colored coins protocol and 2-of-2 multisignature wallets. Lykke exchange and all its tools and services are fully open source.

4. Conclusion

As once formulated by Paul Buchheit: “Bitcoin may be the TCP/IP of money” [13]. The money transmission protocols will evolve and in future there will be many blockchain-based digital assets. The important component that is missing is a global market place that enables exchange of digital assets. Lykke builds such a global internet exchange, where all financial instruments will be traded and exchanged against each other, whatever their asset class or the size of transaction.

The first year of operations of Lykke exchange has shown the viability of the semi-trusted architecture that allows a compromise between usability, liquidity and security of funds in the toxic internet environment.

The transparency of blockchain technology provides unique research opportunities: the trade log has the resolution to participants ID. Potential research directions include in particular:

- Empirical market microstructure of digital assets marketplace and scaling laws;
- Optimal market design;
- Intraday yield curves estimation;
- Market participants ecology and behavioral studies;
- Market abuse detection (wash trades, market price manipulation, etc.); and
- Settlement finality research.

Notes

1. www.bitmaintech.com/productDetail.htm?pid=00020160529072433755 30DcJIoK0654
2. This effect is often referred to as Metcalfe's Law: http://en.wikipedia.org/wiki/Metcalfe%27s_law
3. Market Overview, bitcoincharts.com
4. https://github.com/OpenAssets/open-assets-protocol/blob/master/specification.mediawiki
5. Depends on transaction, see also Maximum Transaction Rate on Bitcoin Wiki.
6. https://blockchain.info/charts/n-transactions
7. https://gist.github.com/gavinandresen/e20c3b5a1d4b97f79ac2
8. http://lightning.network/docs/
9. https://en.bitcoin.it/wiki/Contract#Example_7:_Rapidly-adjusted_.28micro.29payments_to_a_pre-determined_party
10. http://ozlabs.org/~rusty/ln-deploy-draft-01.pdf
11. https://en.bitcoin.it/wiki/Lightning_Network#Hash_locks
12. https://github.com/LykkeCity/LykkeX
13. Paul Buchheit, Creator of Gmail, https://twitter.com/paultoo/status/328969714283995136

References

Nakamoto, S. (2008), "Bitcoin: a peer-to-peer electronic cash system", available at: https://bitco.in/pdf/bitcoin.pdf

Poon, J. and Dryja, T. (2016), "The Bitcoin lightning network: scalable off-chain instant payments", available at: https://lightning.network/lightning-network-paper.pdf

Rosenfeld, M. (2012), "Overview of colored coins", available at: https://bitcoil.co.il/BitcoinX.pdf

Swanson, T. (2015), "Watermarked tokens and pseudonymity on public blockchains", available at: www.ofnumbers.com/wp-content/uploads/2015/11/Watermarked-tokens-and-pseudonymity-on-public-blockchains-Swanson.pdf

Corresponding author
Sergey Ivliev can be contacted at: ivliev@gmail.com